REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
21-04-2017	**Master's Thesis**	**from 08-01-2016 to 06-15-2017**

4. TITLE AND SUBTITLE

The Department of Defense effort to countering the cyberterrorism threat: Is the threat real or hyperbole?

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Lt Col C. L. Alford

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) AND ADDRESS(ES)

National Defense University
Joint Forces Staff College
Joint Advanced Warfighting School
7800 Hampton Blvd
Norfolk, VA 23511-1702

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

N/A

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release, distribution is unlimited.

13. SUPPLEMENTARY NOTES

Not for commercial use without the express written permission of the author.

14. ABSTRACT

There are clear opportunities for DOD to better define and align efforts against counter cyber terror activities using some, but not all elements within the DOTLMPF-P (Doctrine, Organization, Training, Materiel, Leadership and education, Personnel, Facilities and Policy) framework. Specifically, within the Doctrine, Organization, Leadership and Education, and Policy sections of the framework, there exist non-material solitons given the current budgetary challenges faced by the government. The interdependence of USCYBERCOM and USSOCOM in counterterrorism education programs, reciprocal training for the collective defense is both evident and essential to the Homeland.

15. SUBJECT TERMS

Cyber, Terrorism, Cyberterrorism, USSOCOM, USCYBERCOM

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
					Stephen C. Rogers, Colonel, USA **Director, Joint Advanced Warfighting School**
a. REPORT	b. ABSTRACT	c. THIS PAGE			19b. TELEPHONE NUMBER
Unclassified	**Unclassified**	**Unclassified**	**Unclassified/ Unlimited**	**41**	**757-443-6300**

NATIONAL DEFENSE UNIVERSITY

JOINT FORCES STAFF COLLEGE

JOINT ADVANCED WARFIGHTING SCHOOL

The Department of Defense effort to countering the cyberterrorism threat: Is the threat real or hyperbole?

By

C. L. Alford
Lieutenant Colonel, U.S. Air Force

The Department of Defense effort to countering the cyberterrorism threat: Is the threat real or hyperbole?

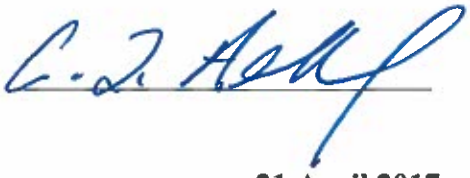
by

C. L. Alford

Lieutenant Colonel, U.S. Air Force

A paper submitted to the Faculty of the Joint Advanced Warfighting School in partial satisfaction of the requirements of a Master of Science Degree in Joint Campaign Planning and Strategy. The contents of this paper reflect my own personal views and are not necessarily endorsed by the Joint Forces Staff College or the Department of Defense.

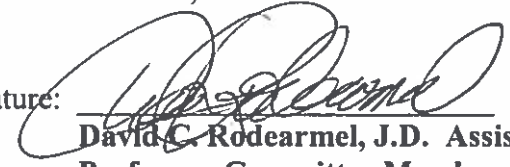
This paper is entirely my own work except as documented in footnotes.

Signature: 

21 April 2017

Thesis Adviser: Signature: 

Stephen Rogers, COL, USA
Thesis Adviser
Director, Joint Advanced Warfighting School

Approved by: Signature: 

David C. Rodearmel, J.D. Assistant Professor, Committee Member

Intentionally left blank

ABSTRACT

Advancements in technology over the last 20 years and the United States' reliance on technology have created unanticipated vulnerabilities. The attacks against government systems continue to trend upward and it is only a matter of time before those threats encroach on critical infrastructure that the nation requires to maintain its security.[1] This journey starts at the whole of government level bringing awareness and understanding of the inherent threats from non-state actors, from both citizens and non-citizens of the U.S., vulnerable infrastructure, and systems. After which the focus narrows to the DOD and the components that need to work closer together to address the complex problem of engaging in counter cyberterrorism in a synchronized coherent manner.

There are clear opportunities for DOD to better define and align efforts against counter cyber terror activities using some, but not all elements within the DOTLMPF-P (Doctrine, Organization, Training, Materiel, Leadership and education, Personnel, Facilities and Policy) framework. Specifically, within the Doctrine, Organization, Leadership and Education, and Policy sections of the framework, there exist non-material solitons given the current budgetary challenges faced by the government.

The interdependence of USCYBERCOM and USSOCOM in counterterrorism education programs, reciprocal training for the collective defense is both evident and essential to the Homeland.

[1] Sellers, John. "Increase in Federal Government Cyber Attacks Lays Groundwork for 2016." Lancope. January 7, 2016. https://www.lancope.com/blog/increase-federal-government-cyber-attacks-lays-groundwork-2016. (Accessed October 21, 2016).

Intentionally left blank

Intentionally left blank

Intentionally left blank

TABLE OF CONTENTS

Intentionally left blank

CHAPTER 1: INTRODUCTION

> *While many hackers have the knowledge, skills, and tools to attack computer systems, they generally lack the motivation to cause violence or severe economic or social harm.*[1] *- Dorothy Denning, Distinguished Professor, Department of Defense Analysis Naval Postgraduate School*

Advancements in technology over the last 20 years and the United States' reliance on technology created unanticipated vulnerabilities that threaten National Security. "Cyber threats to US national and economic security interests are increasing in frequency, scale, sophistication, and severity of impact."[2] Cyber adversaries have escalated their operations to go beyond actions of nuisance and inconvenience. In some instances, they have exploited weaknesses in major information systems and critical infrastructure to create havoc and instill fear. Opinions vary on whether cyberterrorism is a threat, and a lack of verified instances of cyberterrorism attempts, successful or unsuccessful, might support the idea that there is nothing to fear. However, there exist enough evidence to conclude cyberterrorism is a legitimate threat that requires preparation, strategy, and resources to defend against and prevent its potentially devastating consequences.

To demonstrate the complexities of the topic and begin to narrow the focus on the problem, the U.S. must first be aware and understand that there are inherent threats from non-state actors, from both citizens and non-citizens of the U.S., that exploit vulnerable infrastructure and critical systems. Attacks against government systems continue to trend

---

[1] Denning, Dorothy. "Is Cyber Terror Next?" Essays.ssrc.org. N.p., 2001. http://essays.ssrc.org/sept11/essays/denning.htm (Accessed 22 Dec. 2016).

[2] Clapper, James R. "DNI Clapper Opening Statement on the Worldwide Threat Assessment." Office of the Director of National Intelligence. February 9, 2016. https://www.dni.gov/index.php/newsroom/testimonies/217-congressional-testimonies-2016/1314-dni-clapper-opening-statement-on-the-worldwide-threat-assessment-before-the-senate-armed-services-committee-2016. (Accessed October 21, 2016).

upward and it is only a matter of time before those threats encroach on critical infrastructure that the nation requires for maintaining its security.[3] This journey starts at the whole of government level and narrows its focus on the DOD and the commands that need to work closer together to address the complex problem of engaging in counter cyberterrorism in a synchronized coherent manner.

Non-State Actors versus State Actors

Cyberterrorists exist as state and non-state actors. Non-state actors exist as elements or organizations that operate outside of the nation state system, despite the fact that they often live or reside within the boundaries of a nation-state usually without the states' knowledge. Conversely, state sponsored terrorist elements likely reside within the confines of particular state and typically obtain resources covertly and sometimes overtly to conduct terrorist acts designed to influence international outcomes. If a nation-state conducts these acts, it is as an act of war. Whether the nation-state chooses to respond is a choice that is usually consistent with those nation's values. In a kinetic environment, actions are often straightforward with regard to finding and targeting terrorists. However, introducing a non-kinetic threat blurs the lines between non-state and state sponsored actors. Additionally, terrorists' ability to execute operations within the cyber domain in relative anonymity inside any states borders introduces significant complexity to an already complicated problem. Both state and non-state actors pose an equal threat that requires attention.

[3] Sellers, John. "Increase in Federal Government Cyber Attacks Lays Groundwork for 2016." Lancope. January 7, 2016. https://www.lancope.com/blog/increase-federal-government-cyber-attacks-lays-groundwork-2016. (Accessed October 21, 2016).

Human Capital

State and non-state models split cyberterrorists into two distinct categories. There are recruits or members that directly tie to a terrorist group and there are lone wolves who sympathize with a particular cause. In the non-state model, terrorist groups such as the Islamic State in Iraq and Syria (ISIS) actively recruit members with advanced cyber skills to operate within their centralized command structure. This operating technique facilitates three key actions: face-to-face command and control, eyes on cyber talent evaluation, and streamlined decision-making. Maintaining this centralized hierarchy helps to minimize surveillance and detection opportunities for those that might be seeking an operational advantage.[4] Fortunately, this ISIS Cyber unit focuses on nuisance activities like hacking social media accounts on Twitter and Facebook. However, ISIS did cause a disturbance when it hacked U.S. Military social media accounts and exposed their information and advocated sympathizers assassinate the exposed members. The U.S. Military killed the culprit via drone strike, but that did not stop the ISIS effort.[5]

The non-state actor model includes lone wolf actors that are unpredictable by definition and exponentially more difficult to determine what propaganda, knowledge, or event might trigger a sympathetic effort in the cyber domain.[6] The Lone Wolf Cyber actor represents a much greater threat in many respects since a lone wolf can pop up anywhere on the world wide web and certainly disguise their location making attribution

---

[4] Training and Doctrine Command, and U.S. Department of the Army. A Military Guide to Terrorism in the Twenty-first Century. New York, NY: Cosimo, 2010.
[5] Paletta, Damian, Danny Yadron, and Margaret Coker. "U.S. Drone Strike Kills Islamic State Hacker." WSJ. August 26, 2015. http://www.wsj.com/articles/u-s-drone-strike-kills-islamic-statehacker-1440643549. (Accessed November 11, 2016).
[6] Bakker, Edwin, and Beatrice De Graaf. "Preventing Lone Wolf Terrorism: Some CT Approaches Addressed | Bakker | Perspectives on Terrorism." December 2011. http://www.terrorismanalysts.com/pt/index.php/pot/article/view/preventing-lone-wolf/html. (Accessed November 21, 2016).

challenging. A good non-cyber example is the June 12, 2016 Orlando nightclub shooting where an ISIS sympathizer planned and carried out an attack on his own. The perpetrator acted independently without direct guidance from ISIS leadership while professing his act directly supported the ISIS cause.

Applying this model to cyber where a lone actor might use their cyber expertise in the cyber domain to invoke fear, panic, or death using a keyboard and live to do it again, unlike the Orlando nightclub perpetrator. It is doubtful, ISIS leaders within their headquarters issues orders or targets for similar attacks or cyber-attacks to anyone outside that of the controlled group, but that does not lessen the threat.[7]

Both small groups and lone wolf types are present in the state sponsored actor model therefor it is reasonable that a small group can act as a proxy for nation state in an attempt to avoid confrontation with another nation state. In the past, this effort is more closely associated with rebels fighting a guerrilla warfare that likely benefits the nation state sponsoring the effort with weapons or other resources. Although a lone wolf can act on behalf of a nation state, the concept seems contradictory so it would still require an individual to sympathize with the efforts of a nation state to commit a terrorist act.

Countering the two types of cyberterrorist is especially difficult given that those working in close proximity to the organizational leadership are difficult to locate. The terrorists executing as lone wolves are virtually impossible to predetermine unless they conduct significant cyber reconnaissance that opens a door to detection. The actors connected or located with a terrorist leadership Command and Control (C2) node present

[7] Pomerleau, Mark. "ISIS Is Attracting a Loose Cadre of Cyber Warriors -- Defense Systems." Defense Systems. June 5, 2015. https://defensesystems.com/articles/2015/06/05/isis attracts-sympathetic-cyber-warriors-lone-wolves.aspx. (Accessed November 11, 2016).

a certain threat that is more centralized. Conversely, the lone wolves represent the worst of possibilities. These human capitol examples from state sponsored and non-state actor examples illustrate some of the challenges and diversity of the threat that the United States faces in the cyber domain.

Infrastructure and Systems

Infrastructure and computer network systems represent both the weapon and the intended target, which is unusual compared to other operational domains. There is the infrastructure and systems that terrorists use for committing their acts, and there is infrastructure and systems the U.S. is protecting from attack. Predictably, systems virtually connect via billions of connections with anonymity as defense on one side and layered defenses on the other. The connections transcend nation state borders allowing connections from nearly any place on earth to another. As threats or attacks emerge, it is analogous to finding a needle in a haystack when trying to seek and destroy. Meanwhile adversaries can pop-up anywhere to inflict damage or death and disappear (See Figure 1).

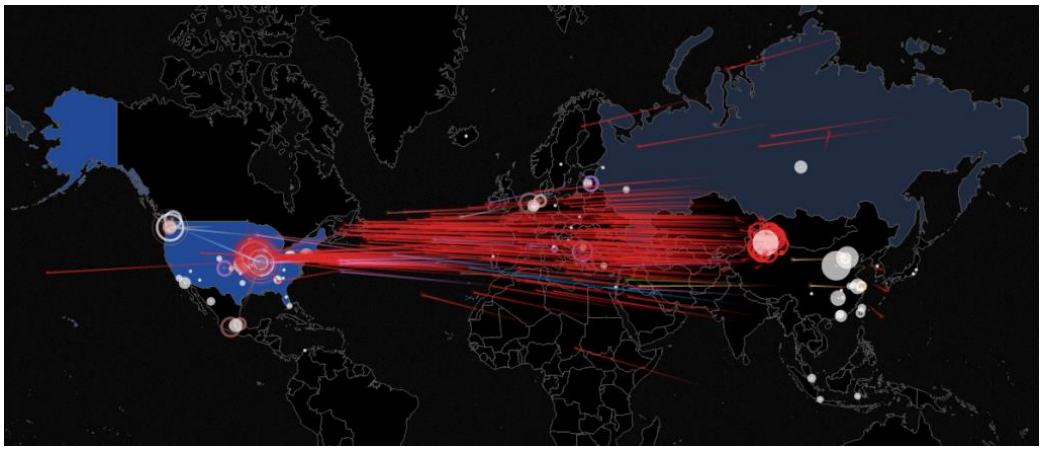


Figure 1: A visualization of Cyberattacks occurring

The U.S. must protect critical infrastructure that compose the assets, systems, and networks, whether physical or virtual. “The systems and infrastructure are so vital that

their incapacitation or destruction would have a devastating effect on security, national economic security, national public health or safety, or any combination thereof."[8] This creates a wide attack surface that terrorists only have to get through once.

On the contrary, a terrorist's attack surface is likely very minimal and may vary between different organizations. A terrorist might yield havoc from a single laptop in their attacks versus a broad system of platforms like those used in the U.S. government. This follows the principles of Mao Zedong's philosophy to wear down a numerically and technologically advantaged adversary.[9] The advantages a large Army has in a traditional force on force war changes quickly when facing asymmetric threats where the large Army provides numerous targets for a much smaller enemy. This viewpoint directly applies to cyberterrorism as the U.S. maintains infrastructure domestically and in more than 180 countries, which can it make it very vulnerable.[10]

Cyberterrorism has become a reality for governments, corporations, militaries, and networks. It is a threat capable of destruction or disruption of service. There is general agreement among cyber experts that cyberattacks can target anyone;[11] these attacks can be disruptive for multiple reasons, which include, but are not limited to destroyed power generation equipment, interrupted environmental controls, and GPS altered Air Traffic control systems. The United States Cyber Command (USCYBERCOM) formed to address such threats by defending Department of Defense

[8] Riedman, David. "How Critical Is Critical Infrastructure? - HOMELAND SECURITY AFFAIRS." HOMELAND SECURITY AFFAIRS. 2015. https://www.hsaj.org/articles/8092. (Accessed November 2, 2016).
[9] Mao, Zedong. On Guerrilla Warfare. New York: Praeger, 1961.
[10] Roberts, Amy. "By the Numbers: U.S. Diplomatic Presence." CNN. May 9, 2013. http://www.cnn.com/2013/05/09/politics/btn-diplomatic-presence/. (Accessed November 27, 2016).
[11] Tucker, Patrick. "Major Cyber Attack Will Cause Significant Loss of Life By 2025, Experts Predict." Defense One. October 29, 2014. http://www.defenseone.com/threats/2014/10/cyber-attack-will-cause-significant-loss-life-2025-experts-predict/97688/. (Accessed November 27, 2016).

(DOD) information networks supporting Combatant Commands (CCMD), and defending the nation. However, United States Special Operation Command (USSOCOM) executes the counterterrorism mission, one of the command's Twelve Core activities. The counterterrorism mission includes actions taken directly and indirectly against terrorist networks to influence and render global and regional environments inhospitable to terrorist networks. Recognizing USSOCOM operations expertise in counterterrorism and the threat of cyberterrorism, the USSOCOM role must evolve to include responsibilities to counter cyberterrorism.

Problem

While the Department of Justice (DOJ) through the Federal Bureau of Investigations (FBI) is the designated lead to protect the United States from terrorist attack, counter-cyberterrorism responsibilities currently overlap several federal agencies: Department of Homeland Security (DHS), Department of Justice (DOJ), and Department of Defense (DOD). Within DOD, terrorism responsibilities split between United States Strategic Command (USSTRATCOM) through its sub-unified command, USCYBERCOM and USSOCOM. USCYBERCOM focuses on countering cyber-attacks while USSOCOM executes a more traditional counterterrorism role, which tends to focus of countering physical threats outside of the U.S. In part, the confusion stems from the variety of interpretations and definitions of key terms, which Chapter 2 addresses in depth.

Thesis Statement

Defending against cyberterrorism is extremely challenging because it must account for the most difficult and dangerous aspects of terrorism, while contending with the complexity and ambiguity of the cyber domain. Each, individually, presents monumental challenges; combined, they present a set of problems that requires a deliberate and focused effort. To maximize effectiveness fighting cyberterrorism, DOD must establish a lead command, illuminate existing operational overlaps, mitigate operational gaps, and reinforce a common cyber domain lexicon similar to the evolution in the traditional kinetic domains of Land, Sea, Air, and Space.

Scope of Research

The aforementioned background serves as essential contextual information for what is clearly a complex problem across the whole of government. This argument focusses on the policy shortfalls, organizational structure vulnerabilities, and challenges that exist in DOD. It highlights areas where vulnerabilities exist that DOD recognized, accepted, and allowed expediency to answer immediate threats within the cyber domain. The research shows expanded relationships within DOD, in line with traditional organizational structures adeptly addresses the current seams between kinetic and non-kinetic special operations activities against the holistic terrorist threat. Both hypothetical and real world scenarios show the range of possibilities. Derivative discussions and references originated from unclassified sources. Research included Official Use Only documents; however, this thesis only references unrestricted information.

Research Methodology

This paper compared and contrasted the roles and responsibilities of existing DOD organizations and policies in accordance with the Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, Facilities and Policy (DOTMLPF-P) model. Specifically, the paper provided an analysis of Doctrinal, Policy, and Organizational overlap, gaps, and challenges within the DOTMLPF-P framework. The research used elements of a Capabilities-Based Assessment that provides enough information to inform a joint DOTMLPF-P Change Recommendation (DCR).[12] A DCR specifically addresses changes to existing joint resources when such changes are not associated with a new defense acquisition program or a non-material solution. This paper serves as an input to the Joint Capabilities Integration and Development System (JCIDS) process that exists to support Joint Requirements Oversight Council (JROC) and Chairman of the Joint Chiefs of Staff (CJCS). CJCS responsibilities include identifying, assessing, validating, and prioritizing joint military capability requirements.[13] The thesis recommends a method by which DOD can organize to prepare for, prevent, and respond to cyberterrorism more effectively.

[12] Department of Defense, Joint Publication 3170.01I, Joint Capabilities Integration and Development System (JCIDS) (Washington, DC: The Joint Staff, 23 January 2015)
[13] Ibid

CHAPTER 2: TERRORISM DEFINITIONS AND POLICY

An element of virtually every national security threat and crime problem the FBI faces is cyber-based or facilitated. We face sophisticated cyber threats from state-sponsored hackers, hackers for hire, organized cyber syndicates, and terrorists.[1]
- James Comey, Director of the Federal Bureau of Investigations

Terrorism and Cybersecurity

An internationally accepted definition of terrorism does not exist at this time and thus the definition of cyberterrorism is equally ambiguous. However, for this paper it is important to focus on the definitions that exist within United States Government under DHS, DOJ, and DOD as it points to the complexity of terrorism internationally and within the whole of government. Each of the aforementioned government agencies have defined terrorism, cybersecurity, and in some cases cyberterrorism. The following are the definitions for each of the respective organizations.

Cybersecurity Definitions

The Cybersecurity Information Sharing Act of 2015 (CISA) tasked DHS and DOJ with implementations of the law. DHS and DOJ recently created a common lexicon of cybersecurity terms for the whole of government and the private sector. For DHS, DOJ, and DOD cybersecurity means the purpose of protecting an information system or information that is stored on, processed by, or transiting an information system from a cybersecurity threat or security vulnerability.[2] This clarity reflects convergence of technology over the last 25 years in everyday life and the need to protect it.

[1] Comey, James. "Threats to the Homeland." FBI. October 08, 2015. https://www.fbi.gov/news/testimony/threats-to-the-homeland. (Accessed December 22, 2016).
[2] Cybersecurity Information Sharing Act of 2015, Sec 105

Terrorism Definitions

Three separate sections of U.S. code: Title 18, title 22, and title 50 address the term terrorism. Title 18 covers crimes and criminal procedures which is applicable to DOJ, Title 22 is foreign relation and applicable to the Department of State, and Title 50 covers War and National Defense and is applicable to DOD.[3] Additionally, under Title 10, the Armed Forces, DOD through USSOCOM performs counterterrorism activities, but there is not a definition within the Title 10 section.

The FBI uses the definition of terrorism from Title 18, and distinguishes between international terrorism and domestic terrorism. Both definitions have three key characteristics. The first two are the same: "Involve violent acts or acts dangerous to human life that violate federal or state law, appear to be intended to intimidate or coerce a civilian population, to influence the policy of a government by intimidation or coercion; or to affect the conduct of a government by mass destruction, assassination, or kidnapping."[4] The location of the act distinguishes the third characteristic: International terrorism occurring outside the territorial jurisdiction of the United States and domestic terrorism occurring inside the territorial jurisdiction of the United States.

DHS garners its definition of terrorism from the Homeland Security Act of 2002. The term terrorism means "any activity that involves an act that is dangerous to human life or potentially destructive of critical infrastructure or key resources, and is a violation of the criminal laws of the United States or of any State. It must appear that the intention is to intimidate or coerce a civilian population, influence the policy of a government by

[3] TITLE 18, Part I, Chapter 1138 § 233; TITLE 22, Chapter 38 § 2656f; TITLE 50, Chapter 36, Subchapter I § 1801
[4] TITLE 18, Part I, Chapter 1138 § 233

intimidation or coercion, or an attempt to affect the conduct of a government by mass destruction, assassination, or kidnapping."[5]

DOS defines international terrorism as terrorism involving U.S. citizens or the territory of more than one country that typically includes premediated and politically motivated acts against non-combatants or U.S. personnel conducting clandestine operations. The DOS definition does not specifically match the other definitions within U.S. code, but meet statutory requirements for reporting and are not intended to meet any other requirements as it pertains to U.S. policy.[6]

DOD defines terrorism as "the unlawful use of violence or threat of violence, often motivated by religious, political, or other ideological beliefs, to instill fear and coerce governments or societies in pursuit of goals that are usually political."[7]

DOJ, DHS, and DOD definitions of terrorism are similar, but not the same. The FBI definition is very broad and considers private property if ideology is behind the act. DHS emphasizes critical infrastructure and actions against that cause mass destruction. The DOD definition is closer to the FBIs version, but as an organization, DOD focuses on countering the threat of terrorism and it is the only one of the three organizations to cite religion as a motivation.[8] The essential element all three-organization definitions have in common with their terrorism definitions is the requirement for violence or the threat of violence. The DOS definition is important, but not relevant as it pertains to conducting counterterrorism activities.

---

[5] PUBLIC LAW 107–296—NOV. 25, 2002 116 STAT. 2135
[6] TITLE 22, Chapter 38 § 2656f
[7] Department of Defense, Joint Publication 1–02, Department of Defense Dictionary of Military and Associated Terms (Washington, DC: The Joint Staff, 8 November 2010, as amended through 15 February 2016, 241.
[8] Department of Defense, Joint Publication 3-26, Counterterrorism (Washington, DC: The Joint Staff, 24 Oct 2014)

Cyberterrorism Definition

Over the last ten to fifteen years, the definition of cyberterrorism has ranged from nonexistent to the nation's most imminent threat.[9] Merriam Webster includes a basic definition "terrorist activities intended to damage or disrupt vital computer systems." At this time, the majority of sources agree that if a cyberterrorism threat exists, it definitely goes beyond the damage or destruction of computer systems. Within the United States government, the National Infrastructure Protection Center (NIPC) under DHS and FBI has similar definitions of cyberterrorism while the DOD does not appear to have a specific definition of cyberterrorism.

The NIPC defines cyberterrorism as "a criminal act conducted with computers and resulting in violence, destruction, or death of targets in an effort to produce terror with the purpose of coercing a government to alter its policies."[10]

The FBI defines cyberterrorism as any "premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant targets by sub-national groups or clandestine agents."[11]

Although the DOD does not have an explicit definition of cyberterrorism, DOD's Cyber Strategy document addresses the threat of terrorist groups and nation states and their ability to cause destruction through cyber-attacks.[12] DOD also has a term called complex catastrophe in which it addresses cyber-attacks and terrorism. Additionally, it is

---

[9] The Cyberterrorism Threat: Findings from a Survey of Researchers, Lee Jarvis, Stuart Macdonald, and Lella Nouri, Studies in Conflict & Terrorism Vol. 37 , Iss. 1,2014

[10] "Cyberterrorism Dictionary Definition | Cyberterrorism Defined." YourDictionary. http://www.yourdictionary.com/cyberterrorism. (Accessed October 05, 2016).

[11] Mudawi Mukhtar Elmusharaf, "Computer Crime Research Center," Cyber Terrorism : The New Kind of Terrorism, April 8, 2014. http://www.crimeresearch.org/articles/Cyber_Terrorism_new_kind_Terrorism. (Accessed October 2, 2016).

[12]Department of Defense, "Special Report: Cyber Strategy." Special Report: Cyber Strategy.. http://www.defense.gov/News/Special-Reports/0415_Cyber-Strategy. (Accessed August 17, 2016)

a viable assumption that a specific definition is not required since the definition of terrorism is encompassing.

DHS and FBI definitions of cyberterrorism both include violence and destruction as prerequisites while DOD relies on its basic definition of terrorism, which extends to the use of cyberspace if it achieves the terrorists desired ends. The definitions appear tailored based on the roles and responsibilities each organization fulfils. DHS's definition of cyberterrorism appears the strongest and least ambiguous, whereas the FBI definition reads as though a terrorist using a bomb to blow up a computer system or a network is an act of cyberterrorism. In some cases, charges of cyberterrorism do not meet the FBIs own definition. For example, the DOJ charged a hacker arrested by the FBI in Malaysia with cyberterrorism for stealing US service member's personal data and passing it to ISIS members. This demonstrates the need for a more consistent, comprehensive definition for the USG.

For consistency, Dorothy Denning's Congressional testimony from 2000 serves as a working definition since it covers all aspects of cyberterrorism:

> Cyberterrorism is the convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear.[13]

This definition of cyberterrorism best discerns the nuances, including the critical components of violence, fear, and political motivation versus inflated inconvenience.

[13] Denning, D. E., "Cyberterrorism," Testimony Before the Special Oversight Panel on Terrorism, Committee on Armed Services, U.S. House of Representatives, May 23, 2000.

Although this definition of cyberterrorism lacks international codification, it is a widely accepted. The definition has stood the test of time as evidenced by DHS's similar but abbreviated definition of cyber terrorism.

CHAPTER 3: COUNTER CYBERTERRORISM GUIDANCE

Policy, legislation, and guidance clearly indicate the importance of cybersecurity and counterterrorism efforts. For Cybersecurity, the most recent guidance exists in the Cybersecurity Act of 2015, the Cybersecurity National Action Plan (CNAP), signed February 2016, and Presidential Policy Directive on US Cyber Incident Coordination (PPD-41), signed July 2016. At present, three key pieces of guidance drive counterterrorism efforts. The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, the Homeland Security Act (HSA) of 2002, and the National Security Intelligence Reform Act of 2004.

A review of these policy, legislation, and guidance documents reveals an overlap in cybersecurity and terrorism; however, cyberterrorism specifics are conspicuously absent. The most significant overlap in terrorism and cybersecurity comes in DHS responsibilities and their required protection of critical infrastructure. This overall bifurcation becomes evident in how the policy and guidance drives the structure of the organizations tasked with countering terrorism and maintaining cyberspace security for the United States. Presently overarching guidance from the White House identifies cybersecurity roles and responsibilities. Each organization, DHS, DOJ, and DOD further identifies their cybersecurity roles and responsibilities that appear to run in parallel to their respective counterterrorism roles and responsibilities.

The White House CNAP directed the Federal Government to establish a cybersecurity environment conducive to enduring improvements within the Federal

Government, the private sector, and the lives of every citizen.[1] A key component of CNAP is deter, discourage, and disrupt malicious activity in cyberspace for which DHS, DOJ, and DOD have direct and indirect, and in some cases overlapping responsibilities.

Another component is enhance Critical Infrastructure Security and Resilience which DHS through NIPC has responsibility. Cyberterrorism is not specifically included in the CNAP guidance, but certainly, the vulnerability of critical infrastructure falls within the cybersecurity threat given proven effects of hostile cyber capabilities such as Stuxnet. [2] Additionally, DHS has the lead for the federal government for securing civilian government computer systems, and works with industry and state, local, tribal, and territorial governments to secure critical infrastructure and information systems. "The Department works to analyze and reduce cyber threats and vulnerabilities, distribute threat warnings, and coordinate the response to cyber incidents to ensure that our computers, networks, and cyber systems remain safe."[3] Again, the term cyberterrorism is not specifically included, but indirectly covers the action if terrorist use cyberspace to commit violent acts as referenced in the DHS definition of cyberterrorism.

September 11, 2001 pushed the United States to establish policy, legislation, and guidance to counter terrorism, including the Homeland Security Act (HSA) of 2002 that established the Department of Homeland Security. More recent cybersecurity policy, legislation, and guidance clearly indicate the importance of addressing and countering the

---

[1] The White House, "Fact Sheet: Cybersecurity National Action Plan", The White House, February 09, 2016. https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan. (Accessed August 21, 2016).

[2] Dan Goodin, "Massive US-planned Cyberattack against Iran Went Well beyond Stuxnet," Ars Technica, February 16, 2016, , http://arstechnica.com/tech-policy/2016/02/massive-us-planned-cyberattack-against-iran-went-well-beyond-stuxnet/. (Accessed October 7, 2016).

[3] "Safeguarding and Securing Cyberspace," Homeland Security. https://www.dhs.gov/safeguarding-and-securing-cyberspace. (Accessed September 7, 2016).

cybersecurity threat to avoid a cyberspace September 11. The intersection of cybersecurity and terrorism policy, legislation, and guidance is not universally clear, but tasked organizations understand the implications.

CHAPTER 4: DOD ORGANIZATIONS

DOD is the largest employer in the world at ~3 Million employees. More than forty sub organizations, made up of Departments, Agencies, Field Activities, and Combatant Commands, comprise the DOD structure (see figure 2).

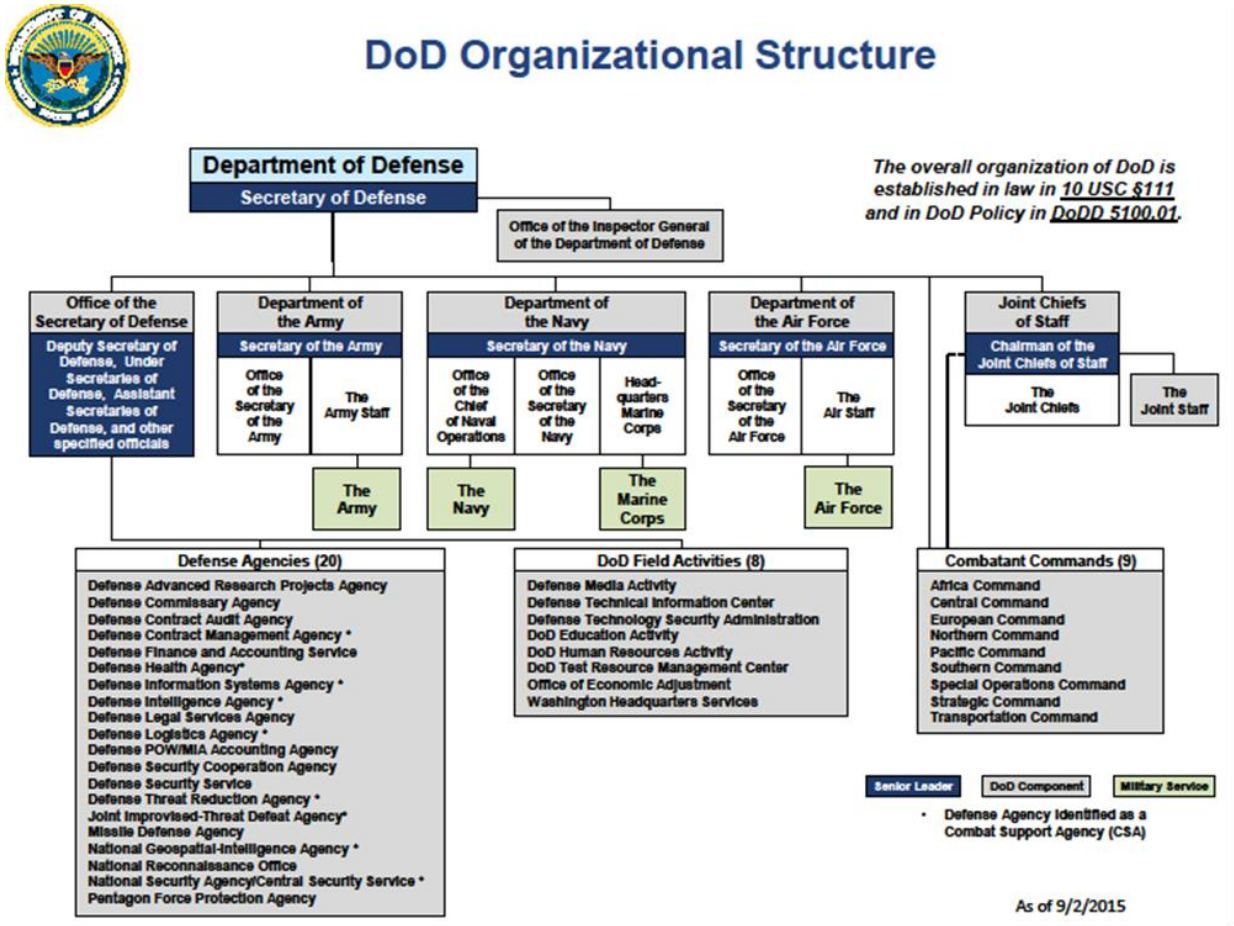


Figure 2 DOD Organizational Structure
http://dcmo.defense.gov/Portals/47/Documents/PDSD/201509_DoD_Organizational_Structure.pdf

The majority of subordinate organizations (likely all) have a role in cybersecurity, but USSTRATCOM is the DOD lead organization through its sub-unified command, USCYBERCOM. Conversely, by law USSOCOM executes Twelve Core activities. One of which is counterterrorism, which includes actions taken directly against terrorist networks (the people). The size of USCYBERCOM, USSOCOM, and the speed at which

their respective threats and activities to counter those threats occur compound the challenges of coordination and information crossflow. These inefficiencies often require reactive efforts after successful terrorist operations. Increasing synergy through organizational realignments or standups with existing personnel may streamline operations and increase the speed required to be effective against cyber terrorism threats. DOD is a huge organization that requires cooperation across all Departments, and Agencies, thus bringing the right elements of USCYBERCOM and USSOCOM together. The combined elements will facilitate more effective counter cyberterrorism efforts that create efficiencies, which is a win for the whole of government and the Nation.

USCYBERCOM

Less than seven years ago the Secretary of Defense (SECDEF) directed the Commander USSTRATCOM to establish a sub-unified command, USCYBERCOM in response to growing cyber threats facing the nation by state and non-state actors.[4] USCYBERCOM plans, coordinates, integrates, synchronizes, and conducts activities to direct the operations and defense of specified Department of Defense information networks (DODIN), prepares for and, when directed, conducts full spectrum military cyberspace operations in order to enable actions in all domains, ensure U.S. /Allied freedom of action in cyberspace, and deny the same to U.S. adversaries.[5] USCYBERCOM uses service elements to help execute their responsibilities, which include Army Cyber Command (ARCYBER), Fleet Cyber Command (FLTCYBER), Air

[4] Reimer, Jordan. "U.S. Cyber Command Preparations Under Way, General Says." Defense.gov News Article: U.S. Cyber Command Preparations Under Way, General Says. March 16, 2010. http://archive.defense.gov/news/newsarticle.aspx?id=58355. (Accessed October 30, 2016).
[5] "U.S. Strategic Command." Components. January 1, 2016. http://www.stratcom.mil/components/. (Accessed December 29, 2016).

Force Cyber Command (AFCYBER) and Marine Forces Cyber Command (MARFORCYBER). Additionally, Coast Guard Cyber Command (CGCYBER), although subordinate to the Department of Homeland Security, has a direct support relationship to USCYBERCOM (see figure 3).

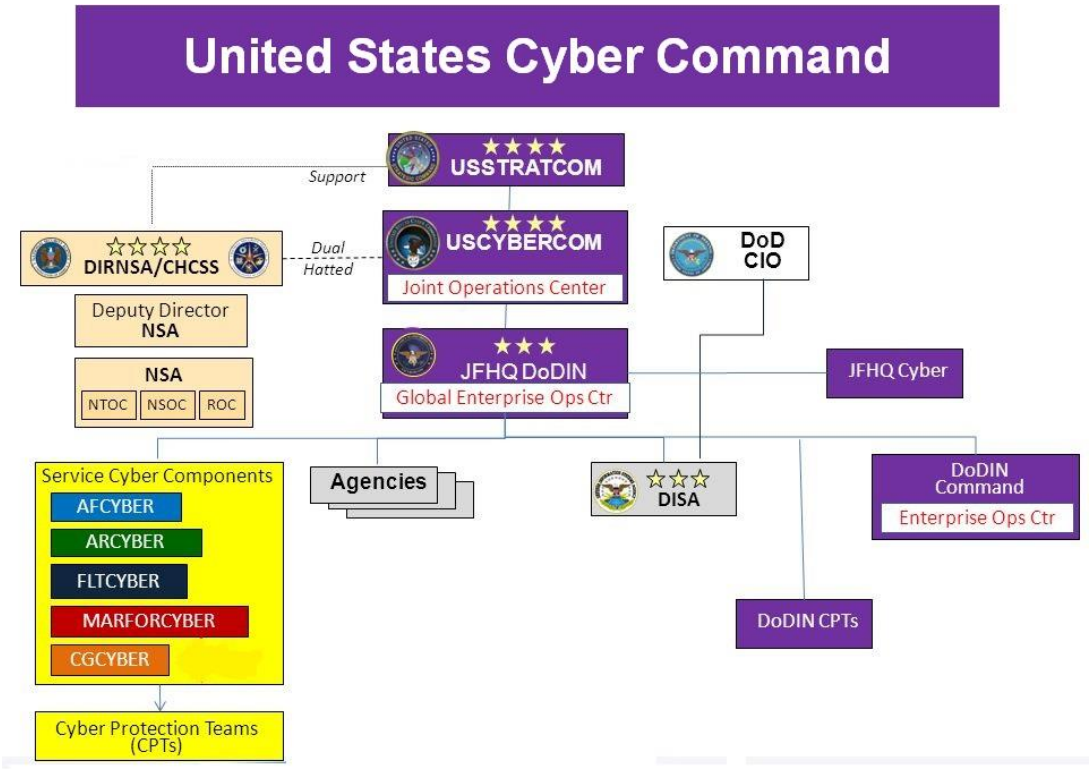


Figure 3: USCYBERCOM Component Support Structure

All one hundred thirty-three of USCYBERCOMs dedicated Cyber Mission Force (CMF) teams achieved initial operating capability as of October 2016 to accomplish the three elements of their mission. The most important one to countering cyberterrorism is strengthening the nation's ability to withstand and respond to cyber-attack.[6]

In support of joint military commander objectives, the services' CMF teams

[6]Department of Defense, "All Cyber Mission Force Teams Achieve Initial Operating Capability," U.S. Department of Defense, October 24, 2016, http://www.defense.gov/News/Article/Article/984663/all-cyber-mission-force-teams-achieve-initial-operating-capability, (Accessed November 29, 2016).

support combatant commands under the Joint Force Headquarters Cyber (JFHQ-C) construct where JFHQ-C MARFORCYBER supports USSOCOM. Although the JFC teams determine roles and responsibilities it is unlikely, the teams focus on National objectives. The National Mission Team (NMT) teams maintain this responsibility, reporting directly to USCYBERCOM, and requires orders from the President to conduct missions. However, JFCs can request NMT support, but that also requires Presidential approval and requires de-confliction against existing priorities at any given time. This represents a major gap in that it creates competition amongst the JFCs for high demand low-density (HDLD) assets. In addition, if the regionally focused JFCs are making Presidential-level approval requests the SECDEF retains the prioritization approval unless otherwise directed.

USSOCOM

The DOD activated USSOCOM almost twenty years ago as part of the Goldwater-Nichols Defense Reorganization Act of 1986 and the Nunn-Cohen Amendment to the National Defense Authorization Act of 1987.[7] Congress mandated a new four-star command be activated to prepare Special Operations Forces (SOF) to carry out assigned missions and, if directed by the President or SECDEF, to plan for and conduct special operations.

Before the September 11, 2001, terrorist attacks on the United States, USSOCOM's primary focus was on its supporting command mission of organizing, training, and equipping SOF and providing those forces to support the geographic combatant commanders and U.S. ambassadors and their country teams. Following 9/11,

[7] Goldwater-Nichols Department of Defense Reorganization Act of 1986 Public Law No: 99-433;

the President further expanded USSOCOMs responsibilities in the 2004 Unified Command Plan (UCP). The UCP assigned USSOCOM responsibility for synchronizing DOD plans against global terrorist networks and, as directed, conducting global operations. USSOCOM receives, reviews, coordinates and prioritizes all DOD plans that support the global campaign against terror and then makes recommendations to the Joint Staff regarding force and resource allocations to meet global requirements.[8] As discussed in chapter 1, USSOCOM executes the counterterrorism mission lead for DOD, which is a critical consideration in an organizational realignment or update of current doctrine and guidance to address this gap.[9]

USSOCOM relies on four components and one sub-unified command to execute the SOF mission set. They include U.S. Army Special Operations Command (USASOC), Naval Special Warfare Command (NAVSPECWARCOM), Air Force Special Operations Command (AFSOC) and Marine Corps Forces Special Operations Command (MARSOC). Additionally, the Joint Special Operations Command (JSOC) is the USSOCOM sub-unified command (See figure 4).

[8] U.S. Special Operations Command, "Mission/Vision/Priorities of U.S. Special Operations Command." http://www.socom.mil/Pages/Mission.aspx. (Accessed September 23, 2016).
[9] Department of Defense, Joint Publication 3-05, Special Operations (Washington, DC: The Joint Staff, 16 July 2014)

Figure 4: USSOCOM Components

USSOCOM also supports the JFCs with six Theater Special Operations Commands (TSOC) respectively: Special Operations Command South, Special Operations Command Africa, Special Operations Command Central, Special Operations Command Pacific, Special Operations Command Europe, and Special Operations Command Korea (SOCKOR) (See Figure 5).

Figure 5 TSOC Areas of Responsibility

Technically, Special Operations Command Korea is a functional command for special operations subordinate to the United States Forces Korea, which is a sub-unified command subordinate to United States Pacific Command. However, the CDR USSOCOM recognizes SOCKOR at the same level as the other Theater Special Operations Commands. Additionally, United States Northern Command (USNORTHCOM) is the only regional Combatant Command that without a TSOC, but does have a USSOCOM element assigned within the USNORTHCOM J3 to meet mission requirements.[10]

USSOCOMs organizational structure is extremely complex and further complicated with operational control maintained by the JFCs. However, regionalized terrorist actors might reside anywhere in the world, thus cyberterrorism challenges this geographic model especially when a lone wolf acts in sympathy. However, USSOCOM must harness the knowledge and understanding of terrorist networks to counter cyberterrorism efforts. Currently, the primary interface between USSOCOM and USCYBERCOM is a single Liaison Officer (LNO), which is not enough.

To streamline SOF reporting to execution in November 2016, the President approved the stand up of a new JSOC task force that reports directly to the Pentagon via USSOCOM. This indicates that gaps clearly existed with the regional model thus this further supports the case of doing something similar with Cyber since it is inherently global in its operations.

[10] McGregor, Otis W., III. "Command and Control of Special Operations Mission in the US Northern Command Area of Responsibility". Master's Thesis, NAVAL POSTGRADUATE SCHOOL, 2005. Monterey, CA: Defense Technical Information Center, Ft Belvoir, VA 2005. 19-20.

CHAPTER 5: DOTMLPF-P

Using the DOTMLPF-P framework to perform a set of tasks to execute a specified course of action for specific standards and situations is essential to establishing ways and means to achieve desired effects. Assessing DOTMLPF-P against current strategic guidance is a proven method to enhance joint force capabilities to or establish new capabilities to meet mission shortfalls.[1] Given the chance of failure or no action due to changing leadership, it is imperative to use this existing framework to ensure relevant analysis and a historical presence for future decision-making regarding the enhancement of counter cyberterrorism efforts within DOD.

In this indeterminate fiscal environment, using the DOTMLPF-P to pursue all options to will close capability gaps and reduce seams is important. However, this chapter focuses on nonmaterial solutions that include changes to doctrine, policy, organization, training, leadership, and education, personnel to reduce or eliminate the need for material solutions. The analysis in this section serves as a platform to set up recommendations that follow in the closing chapter on conclusions and recommendations.

Policy and Doctrine (Joint)

Joint Doctrine consists of fundamental principles by which the military forces or elements thereof guide their actions in support of national objectives. It is authoritative but requires judgment in application.

DOD policy and guidance regarding cyberterrorism crosses joint doctrine and

[1] Chairman of the Joint Chiefs of Staff Instruction, Joint Capabilities Integration and Development System (JCIDS), CJCSI 3170.01I (Washington, DC: The Joint Staff, 23 January 2015)

Office of the Secretary of Defense (OSD) instructions. It includes Joint Publication 3-26, counterterrorism, Joint Publication 3-05, Special Operations, Joint Publication 3-12 (R), Cyberspace Operations, and DoD Instruction 8500.0, Cybersecurity, and DoDI 5240.26, Countering Espionage, International Terrorism, and the Counterintelligence (CI) Insider Threat. By design, DOD level guidance is authoritative, but requires excellent judgment in its execution. As it pertains to countering cyber terrorism specifically, the guidance implies responsibilities, which leads to ambiguity in specific roles and responsibilities within the DOD.

DoD Instruction (DODI) 8500.0 Cybersecurity is very broad in that it indicates DOD IT and DOD information Cybersecurity is an enabler to countering international terrorism without mention of cyberterrorism specifically. DODI 5240.26, Countering Espionage, International Terrorism, and the Counterintelligence (CI) Insider Threat is absent references to counter cyberterrorism and simply places responsibility on the Insider Threat Counterintelligence Group (ITCIG) to coordinate with the DOD Cyber Crime Center (DC3) to monitor for insider threats.

JP 3-26 addresses the Strategic Security Environment. "The strategic security environment is impacted by three dominant strategic themes: globalization and cyberspace technology; political instability; and terrorism and transnational organized crime." This publication clearly addresses the links of a globally connected environment and terrorism and further emphasizes that state actors often use terrorism as form of irregular warfare, which increases the threat. JP 3-26 also recognizes that physical borders or boundaries do not limit terrorist actions just as internal organizational structures should not limit required action to thwart terrorist. The CDR USSOCOM

prepares forces to conduct CT which cyberterrorism inherently links to the task.[2]

JP 3-12, Cyberspace Operations recognizes the ability of transnational actors to execute terrorist acts through cyberspace. JP 3-12 tasks the DOD Cyber Crime Center (DC3) to provide support to agencies tasked with counterterrorism further acknowledging the threat in the environment. Perhaps the most important highlight is the threat of insiders sympathetic to terrorist efforts.[3] Recent insider data leaks portrayed in the news like Eric Snowden, PFC Manning, and Harold Thomas Martin, may seem benign to many. However, the information from these insider breaches offer insight in to the inner workings of the nation's defense against cyber vulnerabilities and a means for terrorist to use previously classified information to defend against them.[4]

This examination of the four DOD and Joint Staff level documents highlights the lack of specificity regarding counter cyberterrorism, but does include implied tasks for USCYBERCOM to work with the Joint Force Commanders' before and during joint operational planning.[5] This implies that USCYBERCOM and USSOCOM relationships already account for reciprocal mission planning at the operational or theater-level, but it also offers significant ambiguity given the overwhelming amount of information that these organizations process. An opportunity exists to update the existing guidance with specified roles and responsibilities within the DOD, required coordination, and better align organization structure to counter the cyber terrorism threat.

---

[2] Department of Defense, Joint Publication 3-26, Counterterrorism (Washington, DC: The Joint Staff, 24 Oct 2014)
[3] Department of Defense, Joint Publication 3-12 (R), Cyberspace Operations (Washington, DC: The Joint Staff, 5 Feb 2013)
[4] Heckman Jory, "Hackers Not Yet Pulling out Big Guns for Data Breaches, NSA Official Warns," FederalNewsRadio.com, October 18, 2016, http://federalnewsradio.com/technology/2016/10/hackers-not-yet-pulling-big-guns-data-breaches-nsa-official-warns/. (Accessed October 20, 2016)
[5] Department of Defense, Joint Publication 3-12 (R), Cyberspace Operations (Washington, DC: The Joint Staff, 5 Feb 2013)

Organization

The analysis examined how USCYBERCOM and USSOCOM task organize to conduct counter cyberterrorism operations in chapter 4. The organizational structure confirmed capability gaps that require attention. These challenges appear in both organizations to include stovepipes, accountable governance, and communications internally and externally between the commands.

Training

USCYBERCOM and USSOCOM have at least two important aspects of training in common. The operators who fulfill personnel requirements in both Combatant Commands have highly specialized training, long lead times to a fully qualified apprentice, and significant recurring currency requirements.

USCYBERCOM depends on the services to provide fully trained operators, but a great deal of specialized training occurs under the National Security Agency (NSA) umbrella. The typical training timeline for an advanced cyber operator is 24 months from accession, which cost thousands of dollars per individual. There is little room for error within the training pipeline to meet sustainment requirements while also considering post qualification attrition rates. Additionally, the respective service-training pipelines that provides input to the more specialized NSA training are unique and lack a common training standard although USCYBERCOM is actively affecting this by establishing Joint Cyberspace Training Standards (JCTS) that include Knowledge, Skills, and Attributes (KSA's). This effort is sure to enhance the skills and readiness of graduating operators

whether it is Defensive Cyber Operations (DCO) or Offensive Cyber Operations (OCO).[6]

USSOCOM training is more daunting and physically demanding in most cases depending upon on the service. Each service brings certain specialties to the SOF team effort whether it is air, sea, or land. However, there is a certain expectation that all forces operating on land are at the same or similar standard physically. Then each service provides certain specialties within the land operations sphere. Air Force provides, Pararescue and Combat Control Teams. The Army provides Rangers, Green Berets, and a Delta Force that accepts personnel from other services. The Navy provides SEALs (Sea, Air, and Land). More recently, the Marines now provide Raiders. Within the specialized units Delta Force and SEAL Team 6s primary mission counter-terrorism and fall under the operational, control of JSOC.[7] The training pipeline is approximately 24 months, with attrition rates between 70-90% across the service programs.

USCYBERCOM and USSOCOM use similar methods to fulfill personnel requirements for their respective mission. Each require highly specialized training lasting more than 24 months with additional training required on a recurring basis to maintain currency in the respective fields. It is unlikely USCYBERCOM operators receive specific training to address the character traits that might enhance the ability to perform counter cyberterrorist actions. It is equally unlikely that SOF forces have specific cyber training to make them more adept at identifying and targeting cyber terrorist.

---

[6] Brickey, Jon, and David Di Tallo,. Cyber Workforce Development, Education, and Training Workshop. Issue brief. iCollege, National Defense University. July 17, 2014. http://icollege.ndu.edu/Portals/74/Documents/Outreach/CYBERBEACON2014WorkshopReportAug2014.pdf. (Accessed October 21, 2016).

[7] Nye, David. "Here are the differences between all the US military's elite special-ops units." Business Insider. May 27, 2015. http://www.businessinsider.com/here-are-the-differences-between-all-of-the-us-militarys-special-ops-units-2015-5. (Accessed October 21, 2016).

Material

The materiel analysis examines the necessary equipment and systems needed by USCYBERCOM and USSOCOM forces to fight and operate effectively and if respective commands require new systems to fill a capability gap. The material section of the DOTMLPF-P model inherently requires funding to meet mission requirements, but often units can meet requirements with non-material solutions working within their existing budget allocations. USSOCOM obtains funding through a separate major force program (MFP), MFP-11. This dedicated source of budgeting and funding occurs to ensure adequate funding independent of the Military Departments, provides visibility into SOF funding from DOD and Congressional oversight as required, and it allows data driven SOF decisions to provide critical capabilities needed to meet current and future national security demands. The USSOCOM FY16 budget came in just under $8 billion with the FY17 budget expected to be approximately $8 billion as well.[8] Conversely, USCYBERCOMs FY16 budget totaled $466 million while the FY17 budget submission requested an increase to $505 million, which is about an 8.4 percent increase.[9] The significant difference in funding between the commands is evident, $7.5 billion; however, USCYBERCOM components bring additional capabilities to bear using their respective service budgeting processes too. Both USCYBERCOM and USSOCOM execute their mission at a high level within their existing budgets and the expectation is that increased

[8] Harrison, Todd. "Analysis of the FY 2017 Defense Budget." A Report of the CSIS International Security Program's Defense Outlook Series . April 2016. http://defense360.csis.org/wp-content/uploads/2016/04/Analysis-of-the-FY-2017-Budget-final-with-cover.pdf. (Accessed November 23, 2016).

[9] Boyd, Aaron. "CYBERCOM gets easiest budget hearing ever." Federal Times. March 16, 2016. http://www.federaltimes.com/story/government/cybersecurity/2016/03/16/house-subcommittee-cybercom/81870980/. (Accessed November 30, 2016).

effectiveness is obtainable with a non-material solution and without any additional funding.

Leadership and Education

This section addresses whether leadership understands the scope and if resources are available to address the issue. The education analysis examines how USCYBERCOM and USSOCOM prepare leaders to lead the fight from the junior operators to the Combatant Commander. The professional development of the joint leader is the creation of a knowledge range that encompasses training, education, and experience.

Training at the operator level is deliberate and extensive for both Commands as discussed in the previously titled section. However, as training prepares operators for their current job, education prepares operators for future jobs through the conveying theoretical concepts and widening the foundation for reasoning and judgment. Educating special operators on the nuances of an asymmetric adversary is fundamental to their success on the battlefield. USSOCOMs Joint Special Operations University (JSOU) list over fifty training courses within their course catalog that prepare SOF to shape the future strategic environment.[10] However, the robust offering is non-inclusive of cyber operations, anti-cyberterrorism, counter cyberterrorism, or any variations resident under communications or intelligence courses as of December 2016. USCYBERCOMs education is much less robust than that of USSOCOM, but Cyberspace Operations is in its infancy compared to a mature USSOCOM or the whole of government counterterrorist organizational efforts. After seven years, USCYBERCOM lacks the foundation

[10] Joint Special Operations University, "Joint Special Operations University Courses." Joint Special Operations University (JSOU). May 29, 2015. https://jsou.socom.mil/Pages/Courses.aspx. (Accessed December 17, 2016).

USSOCOM has regarding education of the cyber force or at least one that synchronizes the educational efforts across the service components. Currently there is not a Cyber University under USSOCOM purview although the ability to obtain graduate level cyber education within the Air Force component and within the National Defense University (NDU) exists. Much like the offerings within the JSOU, the course offerings are limited on any specifics on terrorism, anti-cyberterrorism, counter cyberterrorism, or any variations resident under basic terrorism courses within the curriculum courses. Specifically, the Terrorism and Crime in Cyberspace course offered within the NDU Information Resources Management College (IRMC), which undoubtedly lacks the audience to make a significant impact.[11]

Both USCYBERCOM and USSOCOM rely on extensive experience to grow and mold their operators in to leaders within their respective domains. Obviously, SOF operators execute their mission in situations that are more physically dangerous than Cyber operators are, since SOF executes missions from remote areas of the globe, but the time required to master the tradecraft is similar. Both SOF and Cyber Operations Forces require lucrative DOD bonuses to retain HDLD skills and services to ensure experienced leaders from the junior operator to the commanders.

Training and Education usually interleave when discussing force development, but the purposes relate and serve distinct purposes in the leader development model. Educational opportunities exist within government to expand cross-functional knowledge in terrorisms and cyberspace operations across the two commands. Since both commands

[11] National Defense University, "Information Resources Management College." Cyber Leadership Program. 2016. http://icollege.ndu.edu/Academics/Graduate-Programs/Cyber-Leadership-Program/. (Accessed December 17, 2016).

use highly skilled HDLD personnel through the service components each must continue to seek creative ways to thwart an exodus of highly skilled operators facing pressure from defense contractors and commercial industry that usually offer high salaries and enhanced quality of life for members and their families.

Personnel

The personnel component predominantly ensures that qualified personnel exist to support joint capability requirements. The analysis examines availability of qualified people for a range of military operations and if restructuring closes any capability gaps. This includes the right specialties serving in the right positions at the right time. Both SOF and Cyber service members have long training lead times and fall in to a HDLD category and extensive education requirements before and during service as addressed in training and education sections of this paper. Upon review of raw personnel numbers within a budgetary context, SOF forces have the personnel required to accomplish the mission assigned. Conversely, USCYEBRCOMs personnel availability is less transparent. If judged on CMF capabilities then 133 teams made up of 5000 personnel have reached their Initial Operations Capability (IOC) with half at Full Operational Capability (FOC). The Command goal is to grow the service provided teams by another 1200 personnel within the existing construct by 2018. Although planned increases indicate a shortage of personnel, it is not clear what data the Command or services used to determine 133 teams with 6200 personnel is the right make up. USCYBERCOM is currently conducting a study as of December 2016 called CMF 2.0 to determine if the

force is adequate or if any modifications need to occur as the command moves forward.[12]

Effectively, both commands have trained personnel or have lines of effort to receive trained personnel from their components to meet their joint force mission requirements in peacetime, contingency and wartime operations.

Facilities

The facilities analysis examines military property, installations, and industrial facilities that support military forces to see if they can fill a capability gap. If existing or expanded infrastructure fills a capability gap then its consideration is necessary. To date, USSOCOM and its headquarters components are entrenched within their current locations in Florida, North Carolina, Virginia, and California. USCYBERCOM, although not as mature, shares a similar entrenchment of its headquarters components in Texas, Georgia, Maryland, and Virginia. Any expanded infrastructure likely requires funding which moves it away from a non-material solution. Additionally, a decision on the HQ location for a Sub unified Command or Combatant Command component might drive additional facility considerations. The pending elevation of USCYBERCOM to full combatant command status is a move that likely drives a military construction (MILCON) bill for a new Headquarters. If that comes to fruition, then the location of a new command although assumed as Ft Meade by most, might be better suited at a different location to gain synergy from components. As USCYBERCOM attempts to break free of NSA infrastructure during their status change, it may prove difficult or cost

[12] Pomerleau, Mark. "USCYBERCOM evaluating cyber mission force." C4ISRNET. December 14, 2016. http://www.c4isrnet.com/articles/cybercom-evaluating-cyber-mission-force. (Accessed December 14, 2016).

prohibitive in the near term, but serve the greater good in the long term. This means NSA goes back to providing Intelligence information to key customers on a prioritized basis.

The facility analysis is not a core part of this paper, but changes in organizational structure forces an examination of relevant military property and installations that support the respective combatant forces to see if they can fill an existing capability gap. Fulfilling any requirements in this area drives the proposal from a non-material solution to a material solution.

CHAPTER 6: CONCLUSION AND RECOMMENDATIONS

Today, a shallow planning view against cyberterrorism threats exposes DOD challenges of defending U.S. critical infrastructure when directed by the President. In the absence of a clear guidance and organizational overlap, DOD faces operational inefficiencies easily overcome with little or no funding. DOD should aggressively pursue courses of action to look towards closing seams within the department in order to anticipate and potentially shape the future strategic environment.

Based on the current research and understanding of the problem, there are opportunities for DOD to better define and align counter cyber terror activities efforts for the department using some, but not all elements within the DOTLMPF-P framework. Specifically, opportunities exist within Doctrine, Organization, Leadership and Education, and Policy sections of the framework to enhance, clarify and synchronize cyber operations in support of USSOCOM.

Doctrinally, DOD must update four DOD and Joint Staff level documents that lack specificity regarding counter cyberterrorism. Within *JP 3-26, Counterterrorism*, DOD must clarify implied tasks with regard to tasked support from USSTRATCOM through USCYBERCOM to work with the Joint Force Commanders' before and during joint operational planning. Within *JP 3-12, Cyberspace Operations* DOD must address the possibility of cyberterrorism by transnational actors and further emphasize the insider threat beyond large data breaches. Lastly, *JP 3-05, Special Operations*, indicates cyber operation elements provided to SOF units may require additional training or equipment during special operations missions to support missions effectively and safely. This

highlights the shortfalls in the other two joint pubs and segway's to what the DOD must address within the upcoming Training and Education sections of the framework.

USSOCOMs organizational structure is extremely complex and further complicated with operational control maintained by the JFCs. However, regionalized terrorist actors might reside anywhere on the globe, thus cyberterrorism challenges this geographic model especially when a lone wolf acts in sympathy. USSOCOM must harness the technical knowledge and understanding of terrorist networks to counter cyberterrorism efforts beyond the USSOCOM LNO to USCYBERCOM. Since gaps clearly exist in the regional model and there is a realization by most that cyber operations are inherently global, there are two reasonable organizational options exist:

Option 1 – Stand up a Special Operations Command Cyber Component (SOCCYBER) to USSOCOM (See Figure 6).

Figure 6. SOCCYBER Model

This SOCCYBER element breaks with the current geographic alignment model and is more like Joint Special Operations Command (JSOC) model where additional skills specialized training are concentrated to serve the SOF mission. There is still a question of whether this element is better as a sub unified command under USSOCOM or something similar if USCYBERCOM is elevated to Combatant Command status. If the latter occurs then there is a viable Option 2 - where JFHQ-C MARFORCYBER as lead for support to USSOCOM expands its mission capabilities from support at the headquarters to an expanded presence within USCYBERCOM purview (See Figure 7).

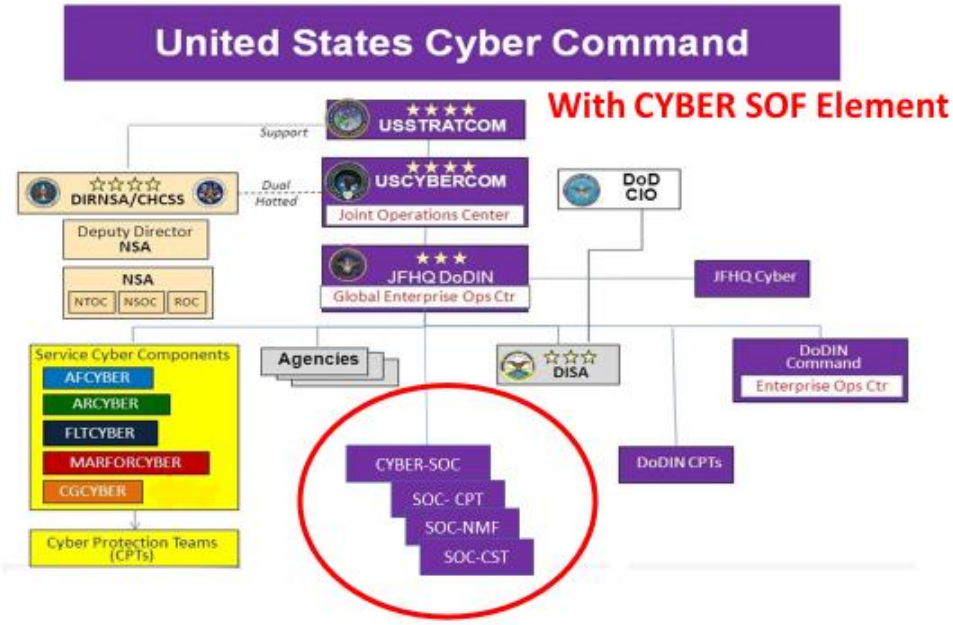


Figure 7: CYBER-SOC Model

USSOCOM Mission requirements would determine whether that equals a Cyber Brigade or Battalion and if a colocation with JSOC at Ft. Bragg is a better placement. Both models would supplant or better augment the Joint Cyber Center and LNO model currently used.

With such an extensive training pipeline for both combatant commands, adding any additional requirements may not provide the most efficient use of time with the substantial attrition rates. However, USCYBERCOM must continue to expand and enforce establishment of JCTSs that include KSA's and fulfill service component requirements.

Education offers a significant opportunity to increase cross-functional knowledge between SOF and Cyber. Within the JSOU, USSOCOM must expand the course offerings to include SOF related nuances of Cyber targets toward CMF Mission tasked to provide Cyber Support to SOF and in most cases making it prerequisite before supporting active SOF missions. Additionally, and preferably within the same educational framework, USCYBERCOM must offer any relevant technical training for SOF members who have opportunities to gain access to disparate networks and expand cyber operations capabilities beyond what may have otherwise been established. If both organizations are at ground zero, benchmarking the DHS "Comprehensive Cyberterrorism Defense" and "The Cyberterrorism First Responder" courses are a good start. The primary goal is a mutual understanding of the respective missions and how one mission can enhance the other at any given time. A secondary goal is cyber operators gain insight into asymmetric adversaries thought process. Both commands can also take advantage of joint professional military education to produce more professionally capable operators.

Policy changes are required from two levels to affect the DOD challenge of countering cyber terrorism in a positive manner. The White House must update its policy enabling DOD to act within an expanded set of authorities, and DOD must update its DoD Instruction 8500.0, Cybersecurity, and DoDI 5240.26, Countering Espionage,

International Terrorism, and the Counterintelligence (CI) Insider Threat. Current White House policy treats cyber operations like a nuclear option except it is actually harder to use than the nuclear option since nuclear use has predetermined options available POTUS can act on within minutes. Establishing a similar framework for Cyber within the classified policy realm will speed the ability for SECDEF to de-conflict and act quickly to counter cyberterrorism threats. Within DOD, SECDEF must further clarify the counter cyberterrorism roles and responsibilities within DODI 8500.0. Within the DoD Cyber Strategy, responsibilities align with USCYBERCOM, but the further codification is required especially since USSOCOM does not have responsibilities within this section. DoDI 5240.26 must assign responsibilities, and provides procedures for counter cyberterrorism activities to counter international threats to DOD and the Homeland.

By adopting some or all of the included proposals, DOD counter cyberterrorism readiness postures will significantly increases. Changes in White House and DOD policy, Joint Doctrine, Education, Organizational structure to eliminate gaps and clarify roles and responsibilities within the counter cyber terrorism operational environment may encourage the service components to pursue the non-duplicative efforts to better prepare their operators for inherently joint endeavors.

The interdependence of USCYBERCOM and USSOCOM in counterterrorism education programs, reciprocal training for the collective defense is both evident and essential to DOD Operations and protection of the Homeland. This analysis is only a glimpse in to what is possible now while the aperture will narrow as USCYBERCOM is elevated to a full CCMD status.

Figures

Bibliography

Bakker, Edwin, and Beatrice De Graaf. "Preventing Lone Wolf Terrorism: Some CT Approaches Addressed | Bakker | Perspectives on Terrorism." December 2011. http://www.terrorismanalysts.com/pt/index.php/pot/article/view/preventing-lone-wolf/html. (Accessed November 21, 2016).

Boyd, Aaron. "CYBERCOM gets easiest budget hearing ever." Federal Times. March 16, 2016, http://www.federaltimes.com/story/government/cybersecurity/2016/03/16/house-subcommittee-cybercom/81870980/. (Accessed November 30, 2016).

Brickey, Jon, and David Di Tallo,. Cyber Workforce Development, Education, and Training Workshop. Issue brief. iCollege, National Defense University. July 17, 2014.http://icollege.ndu.edu/Portals/74/Documents/Outreach/CYBERBEACON2014WorkshopReportAug2014.pdf. (Accessed October 21, 2016).

Broder, Jonathan. "Dr. Strangelove In Cyberspace." Newsweek, Global 167, no. 3 (July 22, 2016): 50-53. Business Source Premier, EBSCOhost (Accessed September 20, 2016).

Chairman of the Joint Chiefs of Staff Instruction, Joint Capabilities Integration and Development System (JCIDS), CJCSI 3170.01I (Washington, DC: The Joint Staff, 23 January 2015).

Clapper, James R. "DNI Clapper Opening Statement on the Worldwide Threat Assessment." Office of the Director of National Intelligence. February 9, 2016. https://www.dni.gov/index.php/newsroom/testimonies/217-congressional-testimonies-2016/1314-dni-clapper-opening-statement-on-the-worldwide-threat-assessment-before-the-senate-armed-services-committee-2016. (Accessed October 21, 2016).

Cybersecurity Information Sharing Act of 2015, Sec 105

Cyberterrorism: the use of the Internet for terrorist purposes. n.p.: Strasbourg : Council of Europe Pub., c2007., 2007. NDU Libraries Catalog, EBSCOhost (accessed September 20, 2016).

David, Jason. Cyber Defense Review. Last modified April 11, 2016. www.cyberdefensereview.org/2016/04/11/cyber-operations-in-2025/. (Accessed August 24, 2016).

Del Quentin Wilber, "Hacker from Kosovo Who Aided Islamic State Is Sentenced to 20 Years in U.S. Prison," Los Angeles Times, September 23, 2016. http://www.latimes.com/nation/la-na-hacker-islamic-state-20160923-snap-story.html. (Accessed October 3, 2016).

Demov, Ivan. "Explaining Cyberterrorism." InfoSec Resources. July 21, 2014. Accessed October 13, 2016. http://resources.infosecinstitute.com/explainingcyberterrorism/.

Denning, D. E., "Cyberterrorism," Testimony Before the Special Oversight Panel on Terrorism, Committee on Armed Services, U.S. House of Representatives, May 23, 2000.

Department of Defense, "All Cyber Mission Force Teams Achieve Initial Operating Capability," U.S. Department of Defense, October 24, 2016, http://www.defense.gov/News/Article/Article/984663/all-cyber-mission-force-teams-achieve-initial-operating-capability, (Accessed November 29, 2016).

Department of Defense, "Special Report: Cyber Strategy." Special Report: Cyber Strategy. Accessed August 17, 2016. http://www.defense.gov/News/Special-Reports/0415_Cyber-Strategy.

Department of Defense, "The Department of Defense Cyber Strategy." DOD. http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf. (Accessed September 6, 2016).

Department of Defense, Joint Publication 1–02, Department of Defense Dictionary of Military and Associated Terms (Washington, DC: The Joint Staff, 8 November 2010, as amended through 15 February 2016, 241.

Department of Defense, Joint Publication 3-05, Special Operations (Washington, DC: The Joint Staff, 16 July 2014)

Department of Defense, Joint Publication 3-26, Counterterrorism (Washington, DC: The Joint Staff, 24 Oct 2014)

Department of Defense, Joint Publication 3-12 (R), Cyberspace Operations (Washington, DC: The Joint Staff, 5 Feb 2013)

Department of Defense, Joint Publication 3170.01I, Joint Capabilities Integration and Development System (JCIDS) (Washington, DC: The Joint Staff, 23 January 2015).

Department of Homeland Security, "Safeguarding and Securing Cyberspace," Homeland Security. https://www.dhs.gov/safeguarding-and-securing-cyberspace. (Accessed September 7, 2016).

Goldwater-Nichols Department of Defense Reorganization Act of 1986 Public Law No: 99-433

Goodin, Dan, "Massive US-planned Cyberattack against Iran Went Well beyond Stuxnet," Ars Technica, February 16, 2016, , http://arstechnica.com/tech-policy/2016/02/massive-us-planned-cyberattack-against-iran-went-well-beyond-stuxnet/. (Accessed October 7, 2016).

Greenblatt, By Mark Lee. "Special Operations Command (SOCOM): Overview." Military.com. Accessed November 13, 2016. http://www.military.com/special-operations/socom-special-operations-command.html

Harrison, Todd. "Analysis of the FY 2017 Defense Budget." A Report of the CSIS International Security Program's Defense Outlook Series . April 2016. http://defense360.csis.org/wp-content/uploads/2016/04/Analysis-of-the-FY-2017-Budget-final-with-cover.pdf. (Accessed November 23, 2016).

Heckman, Jory, "Hackers Not Yet Pulling out Big Guns for Data Breaches, NSA Official Warns," FederalNewsRadio.com, October 18, 2016, http://federalnewsradio.com/technology/2016/10/hackers-not-yet-pulling-big-guns-data-breaches-nsa-official-warns/. (Accessed October 20, 2016).

Jarvis, Lee, and Stuart, MacDinald. 2015. "What Is Cyberterrorism? Findings From a Survey of Researchers." Terrorism & Political Violence 27, no. 4: 657. Publisher Provided Full Text Searching File, EBSCOhost (accessed September 20, 2016).

Joint Special Operations University, "Joint Special Operations University Courses." Joint Special Operations University (JSOU). May 29, 2015. https://jsou.socom.mil/Pages/Courses.aspx. (Accessed December 17, 2016).

Magnuson, Stew. "Cybersecurity." National Defense Industrial Association. Accessed September 1, 2016. www.nationaldefensemagazine.org/archive/2011/August/Pages/DoCyberwarriorsBelongatSpecialOperationsCommand.aspx.

Mao, Zedong. On Guerrilla Warfare. New York: Praeger, 1961.

McGregor, Otis W., III. "Command and Control of Special Operations Mission in the US Northern Command Area of Responsibility". Master's Thesis, NAVAL POSTGRADUATE SCHOOL, 2005. Monterey, CA: Defense Technical Information Center, Ft Belvoir, VA 2005. 19-20.

Mudawi Mukhtar Elmusharaf, "Computer Crime Research Center," Cyber Terrorism : The New Kind of Terrorism, April 8, 2014. http://www.crimeresearch.org/articles/Cyber_Terrorism_new_kind_Terrorism. (Accessed October 2, 2016).

National Defense University, "Information Resources Management College." Cyber Leadership Program. 2016. http://icollege.ndu.edu/Academics/Graduate-Programs/Cyber-Leadership-Program/. (Accessed December 17, 2016).

Nunn-Cohen Amendment to the National Defense Authorization Act of 1987 Sub sec. (e). Pub. L. 100–456

Nye, David. "Here are the differences between all the US military's elite special-ops units." Business Insider. May 27, 2015. http://www.businessinsider.com/here-are-the-differences-between-all-of-the-us-militarys-special-ops-units-2015-5. (Accessed October 21, 2016).

Paletta, Damian, Danny Yadron, and Margaret Coker. "U.S. Drone Strike Kills Islamic State Hacker." WSJ. August 26, 2015. Accessed November 11, 2016. http://www.wsj.com/articles/u-s-drone-strike-kills-islamic-statehacker-1440643549.

Pomerleau, Mark. "ISIS Is Attracting a Loose Cadre of Cyber Warriors -- Defense Systems." Defense Systems. June 5, 2015. Accessed November 11, 2016. https://defensesystems.com/articles/2015/06/05/isis-attracts-sympathetic-cyber-warriors-lone-wolves.aspx.

Pomerleau, Mark. "USCYBERCOM evaluating cyber mission force." C4ISRNET. December 14, 2016. http://www.c4isrnet.com/articles/cybercom-evaluating-cyber-mission-force. (Accessed December 14, 2016).

"Presidential Policy Directive -- United States Cyber Incident Coordination." Whitehouse.gov. https://www.whitehouse.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident. (Accessed September 1, 2016).

PUBLIC LAW 107–296—NOV. 25, 2002 116 STAT. 2135

Reimer, Jordan. "U.S. Cyber Command Preparations Under Way, General Says." Defense.gov News Article: U.S. Cyber Command Preparations Under Way,

Riedman, David. "How Critical Is Critical Infrastructure? - HOMELAND SECURITY AFFAIRS." HOMELAND SECURITY AFFAIRS. 2015. Accessed November 2, 2016. https://www.hsaj.org/articles/8092.

Reimer, Jordan. U.S. Cyber Command Preparations Under Way, General Says. March 16, 2010. http://archive.defense.gov/news/newsarticle.aspx?id=58355. (Accessed October 30, 2016).

Roberts, Amy. "By the Numbers: U.S. Diplomatic Presence." CNN. May 9, 2013. Accessed November 27, 2016. http://www.cnn.com/2013/05/09/politics/btn-diplomatic-presence/

Sellers, John. "Increase in Federal Government Cyber Attacks Lays Groundwork for 2016." Lancope. January 7, 2016. https://www.lancope.com/blog/increase-federal-government-cyber-attacks-lays-groundwork-2016. (Accessed October 21, 2016).

"State, SOCOM Partner to Counter Cyberterrorism | Arthur D. Simons Center." Welcome to the Arthur D. Simons Center for Interagency Cooperation. Accessed August 26, 2016. http://thesimonscenter.org/state-socom-partner-to-counter-cyberterrorism/

Tafoya, William L., Ph.D. "Cyber Terror." Law Enforcement Bulletin. November 15, 2011. Accessed October 7, 2016. https://leb.fbi.gov/2011/november/cyber-terror.

Tanti-Dougall, Rebekah "Cyber Terrorism: A New Threat Against The Maritime Industry." Cyber Terrorism: A New Threat Against The Maritime Industry. July 7, 2014. https://www.lexisnexis.com/legalnewsroom/public-policy/b/public-policy-law-blog/archive/2014/07/17/cyber-terrorism-a-new-threat-against-the-maritime-industry.aspx?Redirected=true. (Accessed November 11, 2016).

TITLE 18, Part I, Chapter 1138 § 233

TITLE 22, Chapter 38 § 2656f

TITLE 50, Chapter 36, Subchapter I § 1801

Training and Doctrine Command, and U.S. Department of the Army. A Military Guide to Terrorism in the Twenty-first Century. New York, NY: Cosimo, 2010.

Tucker, Patrick. "Major Cyber Attack Will Cause Significant Loss of Life By 2025, Experts Predict." Defense One. October 29, 2014. http://www.defenseone.com/threats/2014/10/cyber-attack-will-cause-significant-loss-life-2025-experts-predict/97688/.(Accessed November 27, 2016).

U.S. Special Operations Command, "Mission/Vision/Priorities of U.S. Special Operations Command." http://www.socom.mil/Pages/Mission.aspx. (Accessed September 23, 2016).

U.S. Strategic Command, "U.S. Strategic Command." Components. January 1, 2016. http://www.stratcom.mil/components/. (Accessed December 29, 2016).

The White House, "Fact Sheet: Cybersecurity National Action Plan", The White House, February 09, 2016. https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan. (Accessed August 21, 2016).

The White House, "Foreign Policy Cyber Security." The White House. https://www.whitehouse.gov/issues/foreign- policy/cybersecurity.)Accessed September 6, 2016).

YourDictionary,"Cyberterrorism Dictionary Definition | Cyberterrorism Defined." YourDictionary. http://www.yourdictionary.com/cyberterrorism. (Accessed October 05, 2016).

VITA

Lieutenant Colonel Carlos L. Alford, (USAF) "C. L.," was commissioned into the United States Air Force through Detachment 172, Reserve Officer Training Corps in 1998 following graduation from Valdosta State University with a Master of Public Administration Degree. He is a career Cyberspace Operations Officer with assignments at the Squadron, Group, Numbered Air Force (Mighty Eighth), Headquarters Air Force level and a tour at the White House Communications Agency. Additionally, he has earned a Master's degree in Computer Resources and Information Management from Webster University. He most recently served as Commander, 379th Expeditionary Communications Squadron, Al Udeid AB, Qatar.